# Crypto-World

**Informační sešit GCUCMP**

**ISSN 1801-2140**

**Ročník 7, číslo 6/2005** **15. červen 2005**


# 6/2005

**Připravil: Mgr. Pavel Vondruška**
**Sešit je přednostně distribuován registrovaným čtenářům.**
**Starší sešity jsou dostupné na adrese**
**http://crypto-world.info**
**(855 registrovaných odběratelů)**

**Obsah :** **str.**

# A. Informace pro čtenáře a autory e-zinu Crypto-World

**Mgr. Pavel Vondruška, ČESKÝ TELECOM, a.s.**
(pavel.vondruska@crypto-world.info)

**Přehled:**

- *Crypto-World uzavírá smlouvu s Národní knihovnou o archivaci a katalogizaci svého obsahu*
- *Mikulášská kryptobesídka 2005 – CFP*
- *KEYMAKER 2005 - soutěž o nejlepší studentskou práci*
- *Výzva k rozluštění textu zašifrovaného Enigmou - řešení*

## 1. Crypto-World uzavírá smlouvu s Národní knihovnou o archivaci a katalogizaci svého obsahu

Na základě přidělení ISSN se v oddělení online zdrojů Národní knihovny zabývali hodnocením našeho e-zinu a jeho kategorizací a dospěli k názoru, že splňujeme kritéria projektu Národní knihovny s názvem WebArchiv.

Citace z popisu projektu a výběrových kritérií:

Projekt Národní knihovny s názvem WebArchiv usiluje o získávání, registraci, ochranu, archivaci a trvalé zpřístupnění domácích elektronických online zdrojů. Pro účely tvorby archivu webových zdrojů je třeba aplikovat určitá kritéria výběru tak, aby byly uchovávány dokumenty, jež mají dokumentární hodnotu pro současné i budoucí generace a tvoří národní kulturní bohatství... Více informací o projektu naleznete na http://www.webarchiv.cz/ .

Podepsáním smlouvy jsme dali souhlas k tomu, aby Národní knihovna stahovala a archivovala náš e-zin a poskytovala k němu trvalý veřejný přístup prostřednictvím Internetu. Knihovna ručí za to, že bude dlouhodobě uchováván tak, aby byl přístupný veřejnosti i v tom případě, že průběhem času dojde ke změnám hardwarových či softwarových prostředků, které byly původně použity při vytvoření našeho zdroje. **E-zin bude také zkatalogizován a zařazen do České národní bibliografické databáze a do online katalogu Národní knihovny.**

## 2. Mikulášská kryptobesídka 2005 – CFP

Český a slovenský workshop Mikulášská kryptobesídka (MKB) se bude letos na podzim konat již popáté. Programový výbor tohoto tradičního setkání zveřejnil začátkem června Call for Papers.
Termín podání návrhů příspěvků je stanoven do **12. září 2005.**
Pokyny pro autory a další důležité informace najdete na stránce workshopu: http://www.buslab.cz/mkb/cfp.htm
Workshop se bude konat 1. - 2.prosince 2005.

Mediálními partnery jsou již tradičně náš *e-zin Crypto-World* a odborný časopis *DSM*.

## 3. KEYMAKER 2005 - soutěž o nejlepší studentskou práci

KEYMAKER 2005 je soutěž o nejlepší studentskou práci v oblasti kryptologie a informační bezpečnosti, kterou vypisuje **Brno University Security Laboratory** za podpory firmy **Grisoft, a.s..**

Cílem soutěže KEYMAKER je kromě nalezení největšího *„klíčníka roku“* také podpora studentů vysokých (případně středních) škol v jejich samostatné práci a pomoci jim překonat bariéru odborné a vědecké komunity v České republice. Cílem je také poukázat (především firmám působícím v oblasti IT v České republice), že zde existuje potenciál skvělých mozků, a prokázat možnost většího využití českých škol v řešení konkrétních projektů.

Přijímány jsou články, bakalářské či diplomové práce nebo jiná ucelená díla. Nutnou podmínkou je, aby hlavním autorem podané práce byl student. Nejlepší příspěvky budou otištěny (alespoň ve zkrácené verzi) v našem *e-zinu Crypto-World* a doporučeny k uveřejnění *v časopise DSM*. Vybraní autoři budou prezentovat svou práci na kryptologickém workshopu Mikulášská kryptobesídka 2005. Mezi autory nejlepších prací budou rozděleny ceny v celkové hodnotě 45.000 Kč, které věnovala firma Grisoft.

**Podání návrhů příspěvků: 17. října 2005**
Podrobné informace na http://www.buslab.cz/keymaker

## 3. Výzva k rozluštění textu zašifrovaného Enigmou - řešení

V minulém čísle e-zinu Crypto-World 5/2005 jsme publikovali článek ***Výzva k rozluštění textu zašifrovaného Enigmou.***

Stručně si připomeneme obsah článku. Radioamatérská stanice GB2HQ odvysílala zprávu zašifrovanou pomocí Enigmy. Radioamatéři měli zprávu odchytit, přepsat text jako klasický radiogram a ten dešifrovat.

Připomínám, že zachycené originální vysílání jsme pro zájemce umístili na náš web http://crypto-world.info/casop7/nedele_30m.wav . Pokud nedokážete text radiogramu přepsat, najdete jej v minulém čísle. V závěru článku pak byla zveřejněna výzva k rozluštění tohoto textu. Velice brzy se však ukázalo, že pořadatelé zase až tak přísní na své soutěžící nejsou, neboť zveřejnili konkrétní nastavení Enigmy použité při zašifrování. Poměrně komplikovaný úkol luštění se tím změnil na jednoduchý úkol - text pouze dešifrovat. Nastavení šifrátoru je uvedeno na http://www.princ7.demon.co.uk/method.htm .

Vzhledem k těmto zveřejněným informacím stačí k dešifrování použít vhodný simulátor, nastavit klíče podle výše uvedeného dokumentu a dostanete obsah odvysílané zprávy. Takovým vhodným simulátorem Enigmy je např. ADVANCED ENIGMA SIMULATOR SOFTWARE PROGRAM: (2500 KB) od Dirka Rijmenantse
http://w1tp.com/enigma/#Enigma

Pro ty, kteří jsou zvědaví, co odvysílaný text obsahuje, ale sami se do dešifrování nepustí, zveřejníme otevřený text na naší stránce: http://crypto-world.info/casop7/enigma.txt .
Najdete jej zde však až od 3. července 2005, kdy soutěž vypsaná stanicí GB2HQ končí …

# B. Kontrola certifikační cesty, část 1

**Ing. Petr Rybár, NBÚ SR,** (pr@mailbox.sk)

Text nasledujúceho článku bol v čase publikovania v Crypto-World v procese medzinárodných diskusií s odborníkmi na oblasť elektronického podpisu. Výsledný dokument bude zverejnený na stránkach Slovenského NBÚ http://www.nbusr.sk/NBU_SEP/8.php, aby pomohol pri informovaní odbornej a možno aj laickej verejnosti o základných pravidlách, ktoré sú roztrúsené v rôznych normách, štandardoch a ich súhrnné a ucelené pochopenie je preto v tejto oblasti dosť náročné a tak nasledujúci dokument sa snaží pomôcť k lepšiemu a rýchlejšiemu rozvoju v danej oblasti.

Účelom dokumentu „Kontrola certifikačnej cesty“ je sprehľadniť proces vytvárania a overovania certifikačnej cesty podľa RFC 3280 a požiadaviek kladených pre kvalifikované certifikáty a zaručené elektronické podpisy (Qualified Electornic Signatures).
Správne overovanie certifikačnej cesty je základným predpokladom pre zabezpečenie kompatibility a jednotného prostredia elektronického podpisu v SR s ohľadom na prostredie elektronického podpisu najmä v krajinách EÚ, kde členské štáty zaistia, aby zaručený elektronický podpis (Qualified Electronic Signature) na základe „Article 5, European Directive 1999/93/EC“:

a) uznával rovnaké právne požiadavky na podpis vo vzťahu k údajom v elektronickej forme rovnako ako na vlastnoručný podpis vo vzťahu k papierovým dokumentom
b) bol prijateľný ako dôkaz pri súdnych sporoch.

Snahou autora nebolo vytvorenie samostatného štandardu pre uvedenú oblasť, ale vytvorenie jednoznačného, minimálneho a záväzného profilu pre poskytovateľov certifikačných služieb, tvorcov aplikácií a samozrejme používateľov elektronického podpisu.

Použité definície vychádzajú hlavne z nižšie uvedených štandardov, vyhlášok a zákonov, ktorých definície dokument sumarizuje a upresňuje ich použitie.

Základné dokumenty legislatívy Slovenskej republiky pre elektronický podpis
http://www.nbusr.sk/NBU_SEP/1.php
Formáty zaručených elektronických podpisov. http://www.nbusr.sk/NBU_SEP/8.php

| | | |
|---|---|---|
| RFC 3280 | Internet X.509 Public Key Infrastructure | Apríl 2002 |
| RFC 3739 | Qualified Certificates Profile | Marec 2004 |
| ETSI | TS 101 862 V1.3.2 Qualified Certificate Profile | Jún 2004 |
| ETSI | TS 101 733 V1.5.1 Electronic Signature Formats | December 2003 |
| RFC 3852 | Cryptographic Message Syntax | Júl 2004 |
| ETSI | TR 102 272 V1.1.1 Electronic Signature Policies | December 2003 |
| RFC 3161 | Time-Stamp Protocol (TSP) | August 2001 |

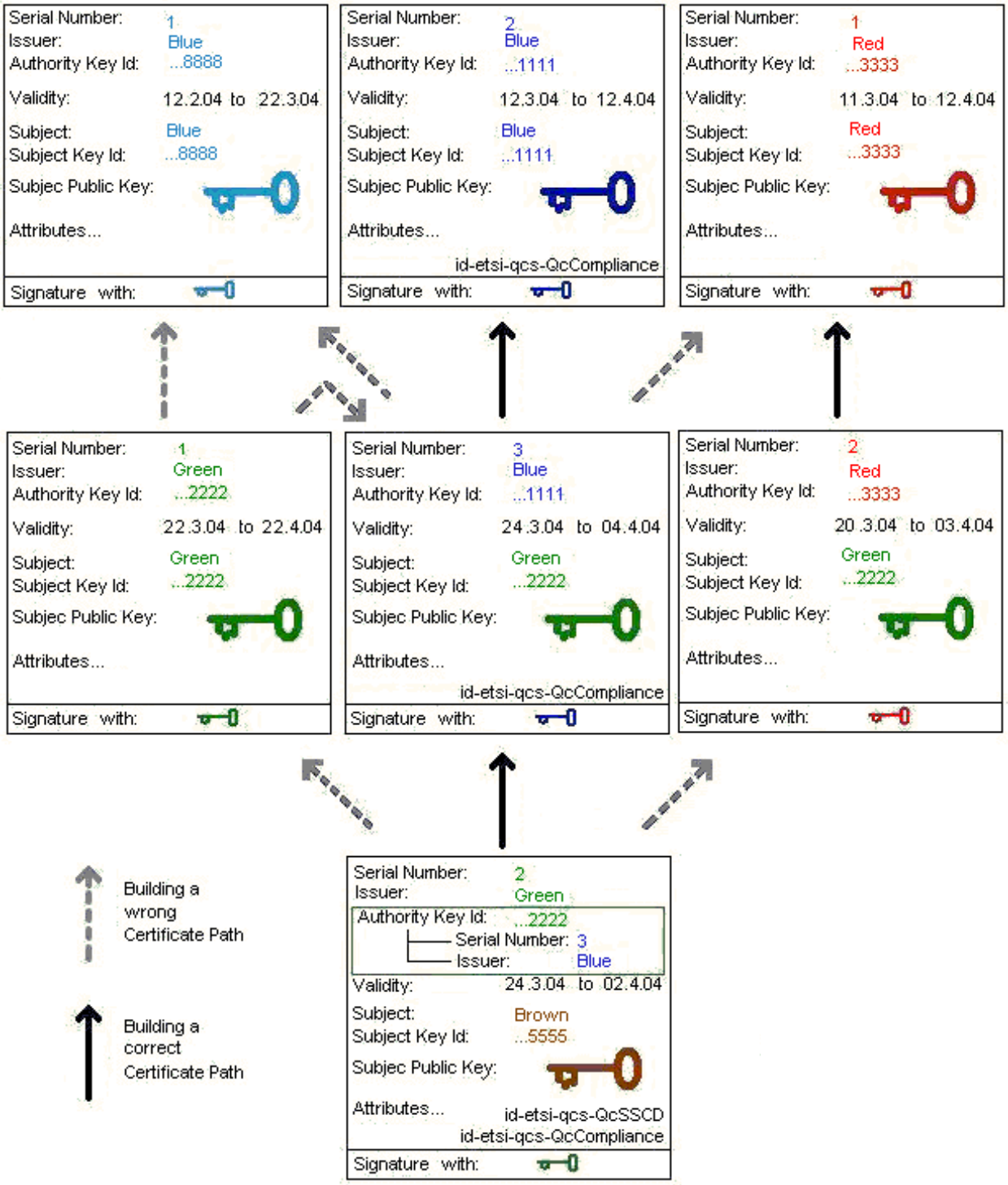
## 1 Príklad certifikačnej cesty a chybných certifikačných ciest

Certifikačné cesty sa zostavujú od koncovej entity až po dôveryhodné koreňové CA z:

- certifikáty koreňových certifikačných autorít: expirovaný certifikát, nový certifikát, ktorý bol vydaný pred expirovaním certifikátu (modrý vlastník - subject a modrý kľúčový pár) a

certifikát nedôveryhodnej (pre overovateľa neznámej) CA (červený vlastník a kľúčový pár)

- *selfSigned* certifikát, certifikát akreditovanej CA a certifikát vydaný nedôveryhodnou CA, lebo červený *selfSign* nemá dôveru overovateľa. V podstate sa môže jednať aj o útok, lebo verejný kľúč je každému dostupný a útočník si môže vytvoriť falošný certifikát, v ktorom podpíše kľúč skutočnej CA, za účelom znemožniť korektné overenie podpisu smerom k dôveryhodnej CA, ak aplikácia nedokáže vybrať správnu cestu s viacej alternatívnych ciest (zelený vlastník a kľúčový pár)
- certifikát koncovej entity - podpisovateľa (hnedý certifikát a kľúčový pár)



Popis chybne zostavených certifikačných ciest, kde certifikát je identifikovaný dvojicou:
( meno vydavateľa certifikátu, sériové číslo certifikátu ).

1. ( Zelený, 2 ) – ( Zelený, 1 ):
   a. nezhoduje sa meno v *AuthorityKeyIdentifier authorityCertIssuer* s menom *Issuer* v certifikáte vydavateľa, „Modry“ ≠ „Zelený“
   b. nezhoduje sa sériové číslo certifikátu v *AuthorityKeyIdentifier authorityCertSerialNumber*, so *serialNumber* v certifikáte vydavateľa, 3 ≠ 1
2. ( Zelený, 1 ) – ( Červený, 2 ):
   a. nezhoduje sa meno v *AuthorityKeyIdentifier authorityCertIssuer* s menom *Issuer* v certifikáte vydavateľa, „Modry“ ≠ „Červený“
   b. nezhoduje sa sériové číslo certifikátu v *AuthorityKeyIdentifier authorityCertSerialNumber*, so *serialNumber* v certifikáte vydavateľa, 3 ≠ 2
3. ( Zelený, 1 ) – ( Modry, 1 ):
   a. nezhoduje sa meno v *Issuer* s menom *Subject* v certifikáte vydavateľa, „Zelený“ ≠ „Modry“
   b. nezhoduje sa v *AuthorityKeyIdentifier keyIdentifier* so *SubjectKeyIdentifier* v certifikáte vydavateľa, ...2222 ≠ ...8888
   c. nepodarí sa overiť podpis certifikátu s verejným kľúčom nesprávneho vydavateľa
   d. vydaný certifikát nie je vydaný v čase platnosti certifikátu nesprávneho vydavateľa
4. ( Modry, 3 ) – ( Modry, 1 ):
   a. nezhoduje sa v *AuthorityKeyIdentifier keyIdentifier* so *SubjectKeyIdentifier* v certifikáte vydavateľa, ...1111 ≠ ...8888
   b. nepodarí sa overiť podpis certifikátu s verejným kľúčom nesprávneho vydavateľa
   c. vydaný certifikát nie je vydaný v čase platnosti certifikátu nesprávneho vydavateľa
5. ( Modry, 3 ) – ( Červený, 1 ):
   a. nezhoduje sa meno v *Issuer* s menom *Subject* v certifikáte vydavateľa, „Modry“ ≠ „Červený“
   b. nezhoduje sa v *AuthorityKeyIdentifier keyIdentifier* so *SubjectKeyIdentifier* v certifikáte vydavateľa, ...1111 ≠ ...3333
   c. nepodarí sa overiť podpis certifikátu s verejným kľúčom nesprávneho vydavateľa

## 2 Pravidlá pre CRL určujúce postup kontroly certifikačnej cesty

**Čas kontroly** je čas, ku ktorému sa overuje platnosť certifikačnej cesty.

- Pri podpise bez časovej pečiatky je to aktuálny čas overovania, ktorý je uložený v bezpečnom auditnom zázname (časová značka) pozostávajúcom minimálne z
  - dôveryhodného času
  - hodnoty, ktorá jednoznačne spája auditný záznam s podpisom, napríklad pomocou HASHu vypočítaného z digitálneho podpisu, ktorý je v elektronickom podpise.
- Pri podpise s časovou pečiatkou je to čas najstaršej platnej časovej pečiatky z digitálneho podpisu, ktorý je v elektronickom podpise.

***CautionPeriod (grace period)*** je časová perióda, ktorá umožní, aby sa informácie o zneplatnení certifikátu spropagovali zneplatňovacím procesom a zverejnili pre overovateľov, teda je to minimálny čas, počas ktorého musí overovateľ čakať od času kontroly, aby získal záväzné informácie o zneplatnení certifikátov a tiež pre poskytovateľov certifikačných služieb, aby tieto informácie o zneplatnení zverejnili.

Teda *cautionPeriod* je čas medzi vydaním dvoch následných CRL, ktorý nesmie presiahnuť čas definovaný legislatívou (24 hodín).

Položka *cautionPeriod* sa nachádza napríklad v podpisovej politike alebo v nastaveniach aplikácií overujúcich certifikačnú cestu.

Čas v CRL ***nextUpdate*** môže byť kratší než je *CRL.thisUpdate + cautionPeriod* a nemusí byť pravidelný v jednotlivých CRL (napríklad o 8 hodín, o 16 hodín).
Pre CRL platí:

- Certifikát v CRL nesmie byť v stave *certificateHold* a *removeFromCRL,* teda jeho platnosť nemôže byť na určitý čas pozastavená.
- CRL nesmie byť vydané po čase *nextUpdate* posledne vydaného CRL.
- Ak je vydané CRL počas platnosti iného CRL, v *nextUpdate* môže byť čas len väčší alebo rovný času *nextUpdate* aktuálne platného najnovšieho CRL. Teda vydané CRL tvoria reťaz.

## 2.1 Prispôsobenie PKI kontrole s CRL slovenskej legislatíve

Pri overovaní podpisov, na základe kvalifikovaných certifikátov vydaných akreditovanými CA podľa platnej legislatívy Slovenskej republiky, je potrebný špecifický postup pri overovaní certifikátu s CRL vydaným na základe PKI, lebo pri vydaní CRL sa terajšími CA nedá technologicky dodržať nižšie uvedená legislatívna podmienka č. 1.:

1. Do ***revocationDate*** pri sériovom čísle zneplatneného certifikátu v CRL sa musí uviesť rovnaký čas, ako je čas vydania CRL, v ktorom bol certifikát prvý krát zneplatnený.

Súčasné CA podľa PKI, sú navrhnuté tak, že prvú podmienku nemôžu zabezpečiť a do *revocationDate* v CRL uvádzajú čas nahlásenia zneplatnenia a nie vydania prvého CRL, teda čas je menší než je čas vydania prvého CRL, v ktorom bol certifikát zneplatnený. Ale aj napriek tomu musí platiť, že do vydávaného CRL sa môže do *revocationDate* uviesť len čas z intervalu **od** *CRL.thisUpdate* aktuálneho posledného CRL **do** času *CRL.thisUpdate* práve vydávaného CRL. Preto algoritmus vyhľadania CRL pre overenie platnosti certifikátu sa rozšíri v prípade zneplatnenia teste pred časom kontroly o vyhľadanie prvého CRL po čase zneplatnenia, ktorý obsahuje sériové číslo zneplatneného certifikátu.

Podmienka overenia certifikátu z certifikačnej cesty podpisu, pomocou CRL:

1. **if** ( certifikát.*notBefore* < *CRL.thisUpdate )* AND
   ( *CRL.thisUpdate* <= certifikát.*notAfter* + *cautionPeriod )* **then**
2. **if** certifikát **is not in** *CRL* **then**
3. **if** ČasKontroly < *CRL.thisUpdate* **then**
   **PLATNÝ**
4. **else**

**NEÚPLNÉ OVERENIE – čakanie na nové CRL**

5. **else**
   **if** ČasKontroly < *CRL*[certifikát].*revocationDate* **then**
   **PLATNÝ**
6. **else**
   **if** ( *CRL.thisUpdate* < ČasKontroly ) OR
   ( *CRL*[certifikát].*revocationDate* < ( ČasKontroly – *cautionPeriod* ) ) **then**
   **NEPLATNÝ**
7. **else**
   **NEÚPLNÉ OVERENIE – žiadosť na CA o prvé CRL so zneplatnením**
8. **else**
   **NEÚPLNÉ OVERENIE – žiadosť na CA o CRL vydané v čase platnosti certifikátu + časový interval, v ktorom je ešte záznam o zneplatnení certifikátu v CRL, aby bolo možné overenie zneplatnenia certifikátu aj tesne pred expirovaní certifikátu.**

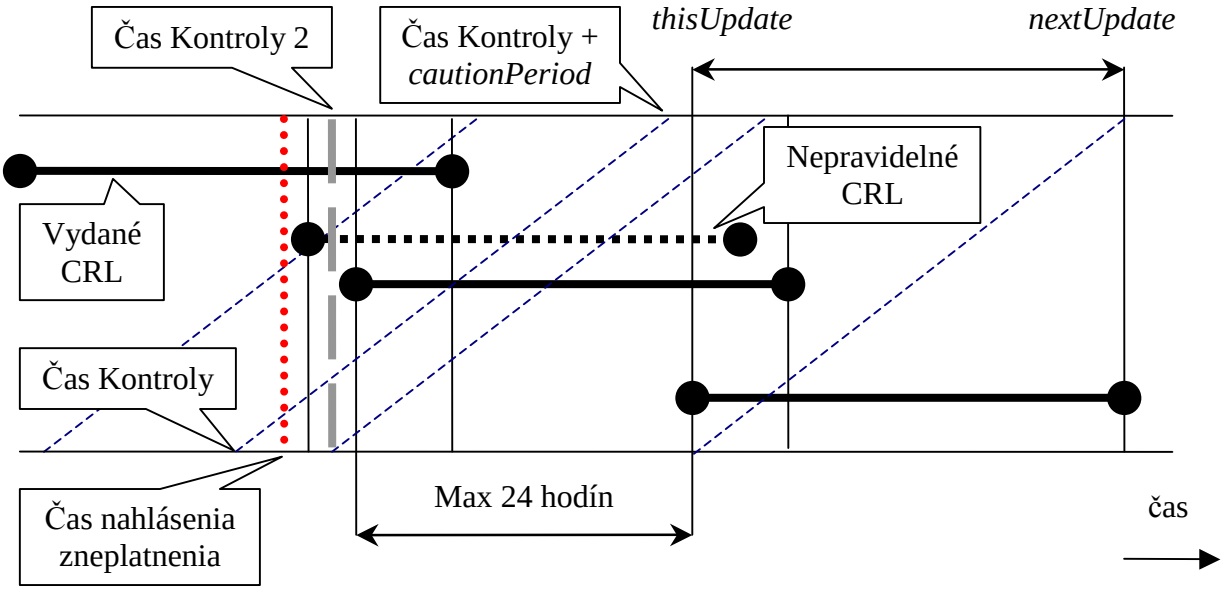
Kde

- *CRL.thisUpdate* je čas vydania CRL
- certifikát.*notBefore* je čas vydania overovaného certifikátu
- a certifikát.*notAfter* je čas, po ktorom certifikát expiruje
- *CRL*[certifikát].*revocationDate* je dátum zneplatnenia certifikátu v CRL

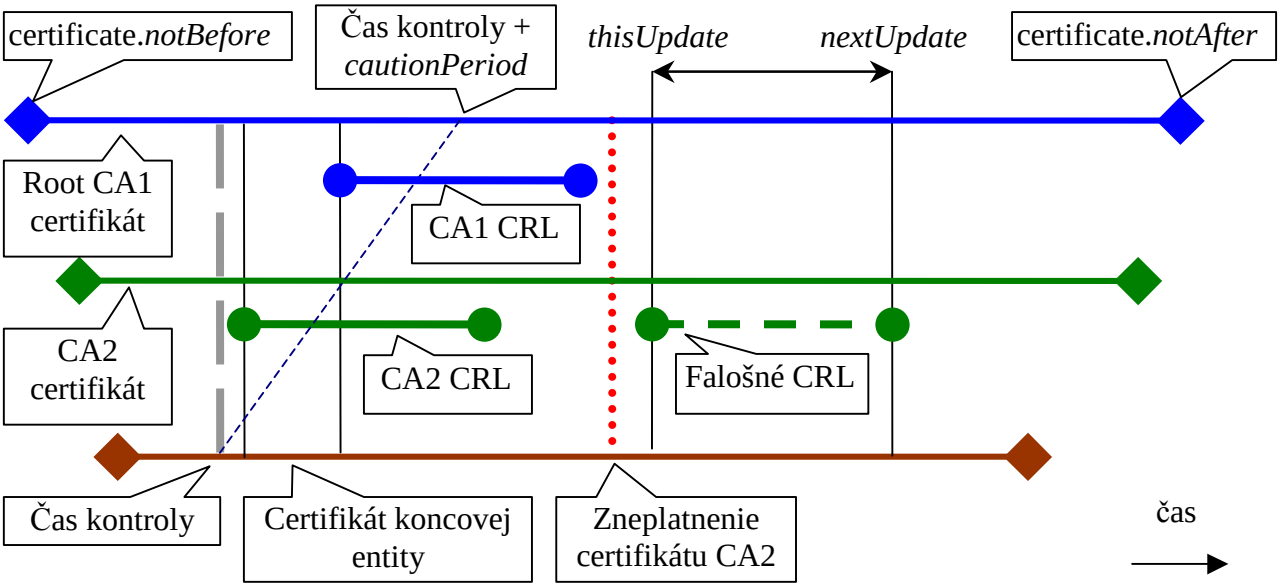
Vysvetlenia k blokom podmienky:

1. CRL je vydané v čase platnosti certifikátu + časový interval, počas ktorého sa záznam o zneplatnení certifikátu nachádza v CRL aj po expirovaní certifikátu (záznam o zneplatnení certifikátu je v CRL minimálne o *cautionPeriod* dlhšie po expirovaní zneplatneného certifikátu)
2. Certifikát nebol zneplatnený, nie je v CRL
3. CRL je vydané po čase kontroly
4. CRL nie je vydané po čase kontroly a treba čakať na nové CRL
5. certifikát bol zneplatnený po čase kontroly, teda je platný
6. certifikát už je dávnejšie zneplatnený v CRL vydanom pred časom kontroly alebo čas zneplatnenia je od času kontroly o *cautionPeriod* skôr a teda nemôže nastať, že prvé CRL, ktoré by zneplatnilo certifikát, by bolo vydané po čase kontroly
7. automaticky sa nedá zistiť či je podpis platný, lebo sa z CA musí získať prvé CRL v ktorom bol certifikát zneplatnený a teda podpisy budú neplatné až od času vydania tohto CRL
8. je potrebné získať CRL, v ktorom sa záznam o zneplatnení môže nachádzať. Podmienka 1.

Pri vyhľadávaní CRL v bode č. 6. sa môže použiť aj *CRLNumber*, ak hodnota *CRLNumber* vo vydaných CRL neprerušene rastie o vopred známu hodnotu alebo CA zverejní formulár pre zadanie zneplatneného sériového čísla certifikátu na vyhľadanie prvej dvojice CRL. Kde v jednom CRL **nebol** certifikát zneplatnený a druhom následnom CRL **bol** certifikát prvý krát zneplatnený. Potom je certifikát neplatný dátumom vydania druhého CRL, ktorý certifikát prvý krát zneplatnil.




Pri kontrole podpisu CRL s certifikátom z certifikačnej cesty a následnej kontrole platnosti certifikátu, ktorým je CRL podpísané, je potrebné splnenie pravidla výberu CRL podľa času vydania CRL.*thisUpdate*. Pravidlo pre výber CRL znie: Pre overenie certifikátov v certifikačnej ceste sa vyberá CRL s časom vydania CRL.*thisUpdate* tak, že každé CRL nadradenej CA je vydané po čase vydania CRL.*thisUpdate* podradenej CA. Je to potrebné kvôli overeniu platnosti podpisu CRL, ktoré je vydané neskôr, než je čas kontroly a teda mohlo dôjsť ku zneplatneniu CA certifikátu, ktorým bolo CRL vydané s hierarchicky nadriadenou CA.




Preto sa tiež na ochranu platnosti všetkých podpisov ktoré CA zrealizovala (certifikáty, CRL, ... ), pred možným zneplatnením CA certifikátu v budúcnosti, použije časové opečiatkovanie celej certifikačnej cesty spolu aj s CRL alebo OCSP. Vďaka opečiatkovaniu sa celá certifikačná cesta spolu s CRL a OCSP môže použiť na overenie dlhodobejšie platných podpisov, aj napriek tomu, že mohlo dôjsť k zneplatneniu CA certifikátu.

## 2.2 Postup kontroly s CRL podľa PKI

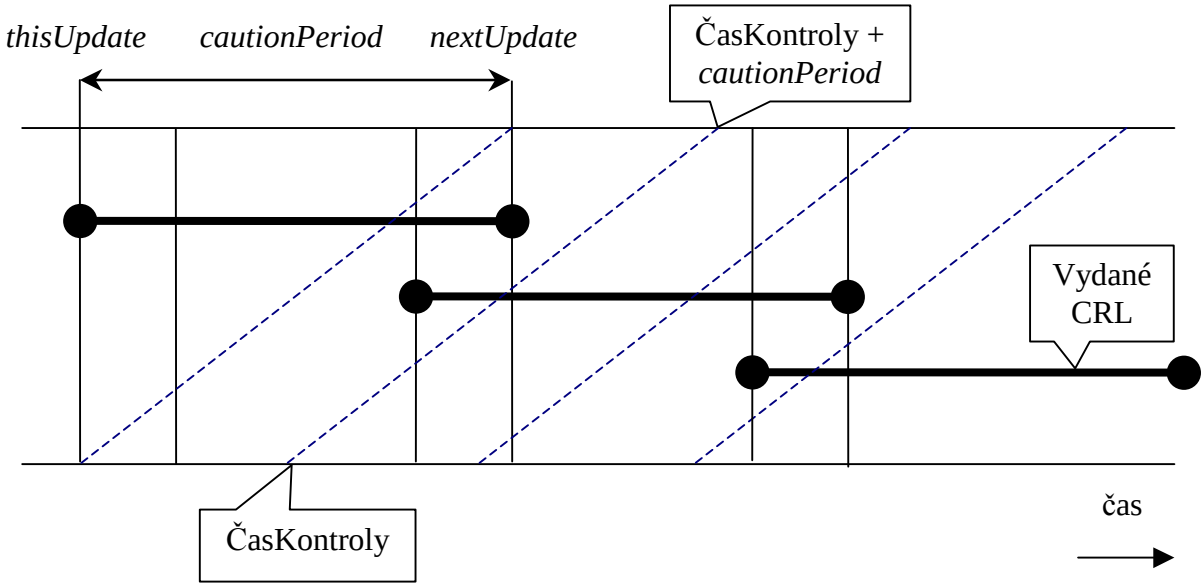
Pri certifikačných autoritách, ktoré nemusia dodržiavať platnú legislatívu Slovenskej republiky (napríklad zahraničná CA), teda pre nekvalifikované certifikáty a kvalifikované certifikáty s položkou *Issuer.countryName* rôznou od „SK“ (Slovensko), sa postupuje nasledujúcim spôsobom pri overovaní podpisov.

1. **if** ( certifikát.*notBefore* < *CRL.thisUpdate* ) AND
   ( *CRL.thisUpdate* <= certifikát.*notAfter* ) **then**
2. **if** certifikát **is not in** *CRL* **then**
3. **if** ( ČasKontroly + *cautionPeriod* ) < *CRL.thisUpdate* **then**
   **PLATNÝ**
4. **else**
   **NEÚPLNÉ OVERENIE – čakanie na nové CRL**
5. **else**
   **if** ČasKontroly < *CRL*[certifikát].*revocationDate* **then**
   **PLATNÝ**
6. **else**
   **NEPLATNÝ**
7. **else**
   **NEÚPLNÉ OVERENIE – žiadosť na CA o CRL vydané v čase platnosti certifikátu (pred expirovaním certifikátu).**

Pri overovaní podpisov a aj pri vytváraní podpisu s úplnou informáciou na overenie, sa doplnia požadované CRL do celej certifikačnej cesty podpisu, ak už nie sú súčasťou podpisu. Teda, aby bolo dostupné požadované CRL, ktoré obsahuje všetky zneplatnené certifikáty, ktoré môžu mať vplyv na platnosť podpisu, musí sa čakať na prvé CRL od času kontroly časový interval *cautionPeriod*.

Vysvetlenia k blokom podmienky:

1. CRL je vydané v čase platnosti certifikátu, teda v čase neexpirovania certifikátu
2. certifikát nebol zneplatnený, nie je v CRL
3. CRL je vydané po čase kontroly + *cautionPeriod*
4. CRL nie je vydané po čase kontroly + *cautionPeriod* a treba čakať na nové CRL
5. certifikát bol zneplatnený po čase kontroly, teda je platný
6. certifikát je zneplatnený v CRL
7. je potrebné získať CRL, v ktorom sa záznam o zneplatnení môže nachádzať. Podmienka 1.




## 3 Porovnanie vydávania CRL podľa zákona o EP a všeobecnej CA

- Podľa zákona o elektronickom podpise, pri overovaní podpisu je potrebné čakať iba na vydanie prvého CRL po čase kontroly a nie celú *CautionPeriod*, lebo zneplatnenie certifikátu nastane až po vydaní prvého CRL, v ktorom sa certifikát nachádza a čas zneplatnenia, bude čas vydania CRL. Pričom čakanie na CRL vydané po čase kontroly nepresiahne *CautionPeriod.*

- Všeobecná CA môže do vydaného CRL vložiť zneplatnený certifikát s časom nahlásenia zneplatnenia, a preto je potrebné čakať na prvé vydané CRL po dobe čas kontroly + *CautionPeriod*. Pretože od nahlásenia do vydania CRL môže uplynúť max *CautionPeriod,* ale v tejto dobe môže dôjsť k vydaniu iných CRL, v ktorých sa zneplatnia iné certifikáty, ale nemusia sa zneplatniť všetky nahlásené. To spôsobuje nepríjemný stav, kedy od **nahlásenia** zneplatnenia certifikátu do **vydania** CRL sú podpisy neplatné, ale nik nemá možnosť zistiť, že podpis je neplatný a je len veľmi ťažko predvídateľné, aké veľké podvody sa môžu zrealizovať počas tejto doby, napríklad v ONLINE aplikáciách. Pomocou OCSP založeného na CRL sa kritická doba iba zmenšuje, ale tiež sa úplne nevyrieši. Preto je odporúčané OCSP, ktoré je založené na záznamoch v databáze. Pre jednoznačnosť OCSP odpovede, OCSP odpoveď musí obsahovať rozšírenie *certHash* definované v ISIS-MTT Optional SigG-Profile. Rozšírenie *certHash* zabezpečuje pozitívnu odpoveď, že systém ktorý vydáva OCSP pozná certifikát (bol vydaný a je v databáze), ktorého stav sa overuje.

V ďalšom čísle si podrobnejšie popíšeme jednotlivé atribúty, ktoré je potrebné pri zostavovaní a overovaní certifikačnej cesty kontrolovať a ukážeme si jednoduché algoritmy na vyhľadanie a overovanie certifikačných ciest, ktoré je možné zostaviť aj cez krížovo certifikované CA certifikáty.

# C. O nezískateľnosti rodného čísla z jeho hashu

**Matej Pivoluska, nezávislý konzultant, MFF UK Praha,**
(pivoluska@matfyz.cz)

## Úvod

Periodicky sa stretávam s návrhom ochrany rodných čísel (ďalej len RČ) pomocou použitia hodnôt ich hashov[1] namiesto samotných RČ. Kryptografické hashovacie funkcie sú okrem iného aj jednosmerné, tj. z hodnoty vypočítaného hashu nie je (v obecnom prípade) možné získať pôvodnú správu. To môže viesť k predstave, že aj z hodnoty hashu RČ nie je možné jednoduchým spôsobom naspäť získať samotné RČ. V nasledujúcom texte bude ukázané, že táto predstava je mylná.

Ak poznáme nasledujúce informácie:

1. typ použitej hashovacej funkcie,
2. presný tvar RČ, v akom sa predáva hash. funkcii na výpočet hodnoty hashu,

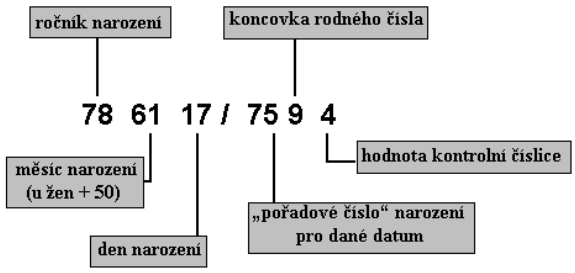
a v bežných prípadoch budú známe (inak by systém nemohol nefungovať), RČ pomocou ich zahashovania neochránime. *Cely problém spočíva v tom, že priestor RČ je proste príliš malý na to, aby odolal tzv. útoku hrubou silou.*

## Priestor RČ

Majme RČ v tvare RRMMDD/KKKK. Toto číslo má 10 číslic v desiatkovej sústave. Naivný horný odhad veľkosti priestoru RČ je $10^{10}$ možných hodnôt.

Zjemnime horný odhad veľkosti priestoru RČ. Povedzme, že sa zaujímame o ročníky 1950–1999. V tom prípade môžu jednotlivé časti rodného čísla nadobúdať nasledujúcich hodnôt:

| | Začiatok | Koniec | Počet hodnôt |
|---|---|---|---|
| RR | 50 | 99 | 50 |
| MM | 01 alebo 51 | 12 alebo 62 | 24 |
| DD | 01 | 31 | 31 |
| KKKK | 0 | 9999 | 10 000 |




1 Kryptografické hashovacie funkcie ako MD5, SHA1, SHA256, etc. Tento článok si nekladie za cieľ vysvetliť, čo je to je to kryptografická hashovacia funkcia. Viac informácií je možné nájsť v bežne dostupnej literatúre alebo napr. na stránkach Wikipedie: http://en.wikipedia.org/wiki/Cryptographic_hash_function

Pre jednoduchosť abstrahujme od faktu, že platné RČ sú deliteľné č. 11. Aj od faktu, že do roku 1953 sa za lomítkom uvádzalo trojčíslie, nie štvorčíslie. Tieto informácie by sa dali využiť na zjemnenie horného odhadu a zrýchlenie výpočtu.

Zjemnený horný odhad veľkosti priestoru možných RČ pre ročníky 1950–1999 je

$|RR| \times |MM| \times |DD| \times |KKKK| = 50 \times 24 \times 31 \times 10\,000 = 372\,000\,000.$

Oproti $10^{10}$ sa podarilo stlačiť horný odhad takmer na tretinu. Ešte stále tu zostáva možnosť tento odhad znížiť, ak prihliadneme aj na deliteľnosť č. 11. To prenechajme ctenému čitateľovi za domáce cvičenie.

Experimentálnemu programu, ktorý počítal v cykle hodnoty hashov pomocou implementácie hashovacej funkcie SHA1 z knižnice OpenSSL, trval výpočet 22 min. Výpočet bežal na počítači s procesorom Athlon XP 1800. Iné hashovacie funkcie budú na tom podobne.

## Bonus

Výpočet je jednoduchým spôsobom lineárne škálovateľný medzi viacero procesorov či počítačov. Priestor RČ sa rozdelí na intervaly a na každom procesore / počítači sa spustí výpočet hash hodnôt len z určitého intervalu. To znamená, ak máme k dispozícii dva počítače, výpočet bude trvať dvakrát menej ako na jednom, ak 10, výpočet bude 10x kratší.

Časovú zložitosť výpočtu tiež neovplyvní počet hľadaných RČ. Hodnoty ich (kryptografických) hashov je možné vložiť do (vyhľadávacej) hashovacej[2] tabuľky, v ktorej je možné vyhľadávať v čase *O(1)*. Reálny čas výpočtu (v sekundách) však zrejme oproti prípadu 1 RČ trochu vzrastie, nebude však ďalej narastať so zvyšovaním počtu hľadaných RČ.

## Záver

Jednosmernosť hashovacích funkcií sme neporušili. My sme ju priam obišli! Čo napokon pri priestore hodnôt správy menšom ako samotný priestor hodnôt dnes bežne používaných hashovacích funkcií ($2^{128}$ až $2^{512}$) nebol veľký problém.

Podobným postupom možno zaútočiť nie len na „zahashované RČ“, ale napr. aj na správy podpísané a zašifrované, ak sú tieto správy dostatočne krátke a máme k dispozícii nezašifrovaný podpis k správe.

2 Nie je hash ako hash.

# D. Přehledová zpráva o významných publikacích a projektech na téma poskytování anonymity, klasifikace a měřitelnost informačního soukromí (privacy), část 2.

**Mgr. Marek Kumpošt,** Fakulta informatiky, MU, Brno
(xkumpost@fi.muni.cz)

*Tato zpráva má za cíl prezentovat dosavadní průzkum v dané oblasti a seznam významných publikací a projektů na dané téma, které jsem pročetl během prvního semestru Ph.D. studia na Fakultě Informatiky.*

*Zpráva je strukturována tak, že ke každé odkázané literatuře je připojen krátký text shrnující problematiku popisovanou v daném článku. V seznamu referencí uvádím veškerou literaturu, tedy i případně tu, která nebude v textu odkázána.*

*V druhé části tohoto přehledu se zaměříme na publikace související s peer-to-peer systémy, měření anonymity, některé teoretické aspekty anonymizačních systémů a útoky na systémy pro poskytování anonymity.*

## Články věnované peer-to-peer systémům

[BG03] se ve svém článku věnuje popisu systému pro poskytování anonymity v GNUsíti – distribuované anonymní a zabezpečené síťování. Hlavní náplní je rozbor protokolu GAP (GNUnet anonymity protocol), což je jednoduchý protokol pro anonymní přenos dat. Smysl GNUsítě je v první řadě poskytovat anonymní sdílení dat mezi uživateli této sítě. Síť podporuje vyhledávání uzlů, autentizaci a šifrování. Veškerá komunikace v síti je důvěrná a pro útočníka tedy nesrozumitelná. Základním cílem projektu je vyhodnocení možností a omezení v prostředí zabezpečeného peer-to-peer síťování. Zajištění anonymity a dalších způsobů ochrany uživatelů je důležité k tomu, aby mohla být síť považována za důvěryhodnou. V GNUsíti neexistuje žádný centrální řídící uzel, neboť ten by se ihned stal terčem útoku. V příspěvku je dále detailně popisován mechanizmus pro poskytování anonymity a další aspekty. Webové stránky projektu mají adresu: http://www.gnu.org/software/GNUnet/.

Článek [FSCM02] představuje systém Tarzan, peer-to-peer anonymitní síťovou vrstvu poskytující IP směrování. Tarzan je flexibilní, decentralizovaný, transparentní a vysoce škálovatelný systém. Tarzan buduje anonymní IP tunely mezi otevřenými uzly. Tarzan může poskytnout anonymitu různým koncovým aplikacím (www, ftp, ssh, VPN, ...) bez nutnosti modifikace těchto aplikací. V úvodu článku je představena architektura a návrh systému Tarzan, budování komunikačních okruhů apod. Následně je diskutována analýza bezpečnosti a anonymity poskytované tímto systémem. V závěru je krátká zmínka o implementaci systému a jeho výkonu.

# Články věnované měření anonymity a teoretickým aspektům

[DSCP03] se zabývá aspekty měření stupně poskytované anonymity. Bere v úvahu fakt, že útočník je schopen získat určitou pravděpodobnostní informaci o uživatelích zkoumaného systému. Stupeň poskytované anonymity je založen na tom, že útočník na základě odposlechnuté komunikace přiřadí různým uživatelům různé pravděpodobnosti toho, že mohli provést danou operaci v systému. V článku je tento model analýzy použit na konkrétní systémy (mixovací systém, zástupy (crowds) a Onion Routing). Je ukázáno, že model je velmi vhodný pro vyhodnocování stupně poskytované anonymity v systému, který je terčem různých typů útoků, že je vhodný pro stanovení míry informace, kterou může útočník v závislosti na zvoleném útoku získat a tento mechanizmus je také vhodný pro vzájemné porovnání různých systémů.

V [KSM03] navrhují dva přístupy pro vyhodnocování anonymity v sítích pro poskytování anonymity. Jeden přístup bere v úvahu komunikační cesty a druhý je brán s ohledem na možnosti volby důvěryhodných aktivních prvků v síti. V příspěvku je pojednáváno o deterministických protokolech a jejich vlivu na míru poskytované anonymity. Nicméně je ukázáno, že je obtížné vybudovat anonymitní síť jenom za použití prostředků deterministického přístupu. V závěru je prezentována simulace s ohledem na prezentovanou problematiku a jsou diskutovány její výsledky.

Článek [KAP02] se zabývá přístupem pro vyhodnocování anonymity, který je založen na anonymitní množině. Ve svém příspěvku se autoři zaměřují na techniky určování anonymitní množiny v otevřených prostředích (typicky Internetu). Autoři se věnují aspektům spojeným s častými změnami subjektů v anonymitní množině a prezentují model umožňující určit míru zabezpečení vybrané anonymizační techniky (např. počet nutných pozorování nebo odposlechů nutných k prolomení některé konkrétní anonymizační techniky). K prezentaci svého útoku používají standardní přístup mixovacích systémů. V úvodu článku prezentují mixovací přístup pro poskytování anonymity jako v současnosti nejběžnější techniku. V další části jsou uvedeny některé pojmy a definice (např. anonymitní množina) a dále je prezentován koncept mixovacího systému. Následně autoři uvádějí formální model mixovacího systému, který používají pro analýzu. V následující sekci je uveden rozbor simulátoru použitého pro analýzu. V závěru jsou uvedeny a diskutovány výsledky provedených simulací.

Aspektům formalizace pojmu anonymity se věnují autoři článku [MVdV04]. Navrhují formální definici anonymity za předpokladu přítomnosti útočníka sledujícího provoz na datových linkách. Dále pak tento navrhovaný formalismus ověřují na vybraném systému – Onion Routing. V úvodu článku je krátce uveden pohled Společných kritérií a jsou zde zmíněny definice pojmů anonymita, nespojitelnost, nesledovatelnost a pseudonymita (zdůrazňují skutečnost, že uvedené definice nejsou žádným způsobem formalizovány). Navrhovaná formální definice je založena na pohledu Společných kritérií a Pfitzmannově definici [PK01]. V úvodu dále zmiňují fungování Onion Routingu a přístup pro vyjádření míry anonymity navrhovaný Diaz et al. [DSCP03]. V další kapitole se autoři věnují formální definici anonymity, v kapitole 3 uvádí formální popis fungování systému Onion Routing v notaci procesní algebry. Předposlední kapitola pojednává o vlastnostech anonymity Onion Routing systému a jsou zde uvedeny některé věty a tvrzení. V závěru pak autoři shrnují dosažené výsledky a diskutují možné směry dalšího výzkumu.

# Články věnované útokům

Aspektům analýzy provozu u konkrétních systémů (the Freedom network a PipeNet) se věnuje [BMS01]. V tomto příspěvku jsou nejdříve popisovány zmiňované dva systémy pro poskytování anonymity při brouzdání na Internetu nebo obecně při použití služeb Internetu, které vyžadují rychlou odezvu. Freedom je systém odolný proti Denial of Service (DoS) útokům, ale je zranitelný vůči některým útokům analýzou provozu. Naproti tomu PipeNet, teoretický model pro poskytování anonymity, je odolný proti útokům analýzou provozu, ale není odolný vůči DoS a některým dalším typům útoků. V článku je diskutován přístup při návrhu systémů, které by byly odolné vůči oběma typům popisovaných útoků.

Dalším článkem diskutujícím útok analýzou provozu a další útoky na systémy poskytující anonymitu je např. [Ray00]. V příspěvku jsou uvedeny základní aspekty útoku analýzou provozu. V úvodních částech je uveden popis různých MIX systémů a jejich základní vlastnosti. Dále následuje poměrně detailní popis dalších typů útoků na systémy poskytující anonymitu. V závěrečné části jsou uvedeny další aspekty související s návrhem mixovacích sítí. Autor též uvádí i možné směry pro další výzkum v této oblasti.

[BL03] se zabývá návrhem metody pro obranu před tzv. *útoky průnikem*. Tyto útoky je možné provést, když není aktivita uživatelů systému rovnoměrná (někteří uživatelé posílají nebo přijímají více zpráv než ostatní). Útočník pak může provést průnik odpovídajících anonymitních množin a získat tak užší výběr možných odesílatelů nebo příjemců dané zprávy. Řešení navrhované v příspěvku se snaží těmto útokům předcházet tzv. *falešným provozem* v síti, kdy síť kromě skutečných zpráv generuje v případě malé aktivity uživatelů umělý provoz, aby zmátla útočníka, který není schopen odlišit skutečné a falešné zprávy v síti.

[DS04] se zabývá útokem na anonymitní systémy využívající statistické metody. Použitím statistických metod může útočník získat (podobně jako při útoku průnikem) určité informace o identitě uživatelů využívajících systém. V příspěvku je podrobně popsaná metoda statistického útoku, který lze použít při útoku na pool mixy. Pool mix je jeden z typů mix systému, kdy má mixovací uzel vnitřní paměť, ve které si uchovává po určitou dobu příchozí zprávy, které v každém běhu mixu zpracuje. V závěru příspěvku jsou uvedeny praktické výsledky popisovaného typu útoku.

V příštím čísle Crypto-Worldu se zaměříme na dvě disertační práce z oblasti anonymizačních systémů a uvedeme několik zbývajících, tématicky nezařazených, článků z oblasti anonymizačních systémů.

# Použitá literatura:

**[BG03]** K. Bennett and C. Grothoff. GAP - Practical Anonymous Networking. *Privacy Enhancing Technologies Workshop (PET 2003)*, LNCS 2760, pages 141-160. Springer-Verlag, 2003.

**[BL03]** O. Berthold and H. Langos. Dummy Traffic against Long Term Intersection Attacks. *Privacy Enhancing Technologies Workshop (PET 2002)*, LNCS 2482, pages 110-128. Springer-Verlag, 2003.

**[BMS01]** A. Back, U. Möller, and A. Stiglic. Traffic Analysis Attacks and Trade-offs in Anonymity Providing Systems. *Information Hiding Workshop (IH 2001)*, LNCS 2137, pages 245-267. Springer-Verlag, 2001.

**[DS04]** G. Danezis and A. Serjantov. Statistical Disclosure or Intersection Attacks on Anonymity Systems. *International Workshop, (IH 2004)*, LNCS 3200, pages 293-308. Springer-Verlag, 2004.

**[DSCP03]** C. Díaz, S. Seys, J. Claessens, and B. Preneel. Towards Measuring Anonymity. *Privacy Enhancing Technologies Workshop (PET 2002)*, LNCS 2482, pages 54-68. Springer-Verlag, 2003.

**[FSCM02]** M. J. Freedman, E. Sit, J. Cates, and R. Morris. Introducing Tarzan, a Peer-to-peer Anonymizing Network Layer. *Peer-to-Peer Systems: First International Workshop, IPTPS 2002*, LNCS 2429, pages 121-129. Springer-Verlag, 2002.

**[KAP02]** D. Kesdogan, D. Agrawal, and S. Penz. Limits of Anonymity in Open Environments. *Information Hiding Workshop (IH 2002)*, LNCS 2578, pages 53-69. Springer-Verlag, 2002.

**[KSM03]** S. Kitazawa, M. Soshi, and A Miyaji. Evaluation of Anonymity of Practical Anonymous Communication Networks. *ACISP 2003*, LNCS 2727, pages 13-26. Springer-Verlag, 2003.

**[MVdV04]** S. Mauw, J.H.S. Verschuren, and E.P. de Vink. A Formalization of Anonymity and Onion Routing. *ESORICS 2004: 9th European Symposium on Research in Computer Security*, LNCS 3193, pages 109-124. Springer-Verlag, 2004.

**[PK01]** A. Pfitzmann and M. Köhntopp. Anonymity, Unobservability, and Pseudonymity - A Proposal for Terminology. *Anonymity 2000*, LNCS 2009, pages 1-9. Springer-Verlag, 2001.

**[Ray00]** Jean-François Raymond. Traffic Analysis: Protocols, Attacks, Design Issues, and Open Problems. *Anonymity 2000*, LNCS 2009, pages 10-29. Springer-Verlag, 2000.

# E. Kryptografické eskalační protokoly, část 1.

**Jan Krhovják,** Fakulta informatiky, MU, Brno
(xkrhovj@fi.muni.cz)

*V této části se seznámíme se základními vlastnostmi kryptografických eskalačních protokolů, s možnostmi jejich nasazení a s principy a problémy návrhu prvních eskalačních protokolů. V dalších částech se pak budeme věnovat jak jejich různým modifikacím a zlepšením, tak také dalším (zcela odlišným) typům protokolů. Cílem tohoto seriálu není podat vyčerpávající přehled ani přesný a úplný popis všech eskalačních protokolů, ale spíše informovat o některých poměrně zajímavých protokolech (a bezpečnostních problémech, které musely být při jejich návrhu zváženy a vyřešeny).*

## Motivace

V dnešní době, kdy se počítače stávají běžnou součástí každodenního života a elektronické obchodování již není jen předmětem teoretických rozprav několika nadšenců v akademické sféře, je vzdálená autentizace uživatelů naprosto klíčovým faktorem mnoha používaných systémů a potřeba kvalitních a bezpečných autentizačních protokolů vzrůstá každým dnem stále více.

K velmi oblíbené metodě autentizace uživatelů patří použití nějaké tajné, krátké, a tudíž i snadno zapamatovatelné informace, jako je například PIN či heslo, jejíž znalostí prokazuje uživatel svou identitu. Naneštěstí klasické kryptografické protokoly navržené pro vzdálenou autentizaci vyžadují použití kvalitních a předem ustavených kryptografických klíčů, které bývají dlouhé řádově stovky bitů a pro člověka jsou zcela nezapamatovatelné.

Využití krátkých PINů či hesel v těchto protokolech bylo dlouhou dobu pokládáno za nemožné, protože jejich verifikace přes nezabezpečený kanál je vždy vystavovala riziku slovníkového útoku. Počátkem devadesátých let minulého století však bylo objeveno několik metod, jak se tohoto útoku vyvarovat. Vznikla nová třída autentizačních tzv. eskalačních protokolů, které byly založeny pouze na použití PINů či hesel a umožňovaly navíc i ustavení kvalitních kryptografických klíčů.

Protože po uživateli je celkově vyžadována jen znalost nějaké tajné informace, jsou tyto protokoly snazší a méně náročné při zavádění do praxe, něž například metody založené na použití biometrik či tokenů. Tam kde již nějaká forma bezpečnostní infrastruktury existuje, může dodatečná implementace těchto protokolů sloužit jako další nezávislý autentizační mechanizmus, který významně přispěje a posílí zabezpečení systému jakožto celku.

Praktická aplikace tohoto typu protokolů pokrývá veškeré případy komunikace přes nezabezpečený kanál, kde by dlouhotrvající uchovávání kryptografických klíčů bylo nebezpečné či nepraktické. Příkladem může být jejich nasazení v dnes poměrně rozšířeném autentizačním sytému Kerberos, ale také použití jako náhrada zastaralých internetových protokolů umožňujících vzdálený login pomocí hesel zasílaných v otevřené podobě. Zajímavou aplikací může být i zabezpečení vzdáleného přístupu ke kryptografické čipové kartě podporující technologii Java Card™ či vytvoření efektivnějšího modelu budoucích sítí bankomatů, kde by již autentizace pomocí zákazníkova PINu neprobíhala přes několik mezilehlých síťových přepínačů sdílejících stejné předem ustavené tajné šifrovací klíče.

# Úvod a terminologie

Zajímavý způsob vytváření (a distribuce) kvalitních kryptografických klíčů nám nabízejí některé kryptografické protokoly. Jejich typickým příkladem je známá Diffie-Hellmanova (DH) metoda ustavení klíčů [DH76], kde sdílený klíč vzniká na základě náhodných dat vygenerovaných oběma stranami.

Chtějí-li si dvě strany[3] protokolu ustavit sdílený klíč sezení, domluví se nejprve nějakým způsobem na velkém prvočíselném modulu $\beta$ a na generátoru $\alpha$ multiplikativní grupy $Z_\beta^*$ Obě tyto hodnoty jsou veřejné[4] a jako $\beta$ je doporučeno volit *bezpečné prvočíslo* tvaru $\beta = 2\gamma + 1$, kde $\gamma$ je velké prvočíslo [PH78, vOW96]. Poté si přes nezabezpečený kanál zašlou následující zprávy (někdy označované jako *DH hodnoty*):

| A | | B |
|---|---|---|
| $\alpha^{rA} \bmod \beta$ | $\rightarrow$ | |
| | $\leftarrow$ | $\alpha^{rB} \bmod \beta$ |
| | … | |

Čísla *rA* i *rB* jsou jednotlivými stranami generovány náhodně[5] z intervalu $\langle 2, \beta - 1 \rangle$. Sdílený klíč sezení $K_S$ je pak každou stranou získán tak, že je přijatá DH hodnota umocněna na náhodně vygenerované číslo příslušné strany a $K_S = \alpha^{rArB} \bmod \beta$.

Nedostatkem tohoto protokolu je zranitelnost útokem typu *man in the middle*. Tento problém řeší autentizované verze protokolu [DvOW92], které umožňují vzájemné ověření identity jednotlivých komunikujících stran (avšak vyžadují k tomu předem ustavené kryptografické klíče, certifikáty apod.).

My se v dalším zaměříme především na tzv. *eskalační protokoly*, které jsou založeny na použití dat s nízkou entropií (jako například hesel). Tyto kryptografické protokoly náleží k mimořádné třídě metod, které zajišťují autentizované ustavení klíčů přes nezabezpečený kanál a jsou založeny na použití hesel způsobem, který je nevystaví riziku off-line útoku hrubou silou (a tedy ani slovníkovému útoku). Jako eskalační je nazýváme proto, že málo kvalitní hesla eskalují na kvalitní kryptografické klíče.

Pokud neřekneme jinak, budeme předpokládat, že obě strany protokolu (tj. klient i server) mají předem ustaveno společné tajné heslo. Při vlastním popisu protokolů budeme také velmi často vynechávat zasílané identifikátory jednotlivých stan (ačkoliv jejich opomenutí by v reálných implementacích mohlo vést k nejrůznějším útokům). Šifrování (a dešifrování) budeme značit jako $E_K$ (a $D_K$), kde $K$ je použitý klíč. Bude-li $K$ tajný symetrický klíč, bude i šifrování/dešifrování prováděno nějakým symetrickým algoritmem. Bude-li $K$ jeden z páru veřejný/soukromý klíč, bude i šifrování/dešifrování (resp. verifikace/podepisování) prováděno nějakým asymetrickým algoritmem.

[3] Většinou je budeme označovat pojmy *strana A* a *strana B*. Při použití terminologie klient/server, pak bude strana A chápána vždy jako klient a strana B jako server.

[4] Při popisu tohoto či jemu podobných protokolů budeme předpokládat, že již byly ustaveny.

[5] Předpokládáme tedy na obou stranách existenci kryptograficky bezpečného generátoru (pseudo)náhodných sekvencí/čísel.

# (DH)EKE

Historicky první protokol spadající do této kategorie je označován jako *EKE (encrypted key exchange)* [BM92] a jedná se o zcela originální kombinaci asymetrické a symetrické kryptografie. Základní část protokolu vypadá následovně:

| A | | B |
|---|---|---|
| $E_P(VA)$ | $\rightarrow$ | |
| | $\leftarrow$ | $E_P(E_{VA}(K_S))$ |
| | … | |

Sdílený tajný klíč (v tomto případě tedy heslo *P*) je použit k zašifrování veřejného klíče strany A (z jednorázově vygenerovaného páru soukromý/veřejný klíč), který je v zašifrované podobě doručen straně B, dešifrován a použit spolu s heslem k zašifrování touto stranou jednorázově vygenerovaného klíče sezení. Ten je pak odeslán zpět straně A a pomocí hesla a soukromého klíče dešifrován. V další části protokol pokračuje výměnou několika klíčem sezení zašifrovaných zpráv, které zajišťují ochranu proti útokům přehráním (např. pomocí náhodných čísel či časových razítek) a ověřují, zda ustavení klíče sezení proběhlo korektně.

EKE může být použit jak se systémy umožňujícími distribuci veřejného klíče (obzvláště dobře funguje s DH metodou ustavení klíčů [DH76]) tak s asymetrickými kryptosystémy (po vyřešení specifických problémů lze použít například RSA či ElGamal). Z bezpečnostního hlediska je u tohoto protokolu zcela zásadní, aby zpráva, která má být pomocí hesla zašifrována (např. výše zmíněný veřejný klíč), byla nerozlišitelná od náhodného čísla. V opačném případě (tj. kdyby zpráva měla určitou strukturu, kontrolní součet apod.) by bylo snadné provést off-line útok hrubou silou.

Při implementaci EKE pomocí RSA není například možné efektivně zakódovat veřejný klíč (*n*, *e*) tak, aby byl nerozlišitelný od náhodného čísla – útočník může vždy testovat, zdali má modulo *n* malé prvočíselné dělitele. Proto může být pomocí hesla zašifrován pouze exponent *e*, ke kterému je ještě před zašifrováním s pravděpodobností 1/2 přičtena hodnota *1* (protože všechny přípustné hodnoty *e* jsou liché). Implementace založená na kryptosystému ElGamal tímto nedostatkem netrpí, protože veřejné klíče jsou zde generovány jako $\alpha^r \bmod \beta$ a mají tedy rovnoměrné rozložení na intervalu hodnot $\langle 1, \beta - 1 \rangle$.

Kdybychom u výše uvedeného příkladu s RSA ponechali před zašifrováním exponenty vždy liché, mohl by útočník při každém pokusu o dešifrování $E_P(VA)$ pomocí zkoušených hesel *P'* zredukovat prostor možných hesel přibližně na polovinu. Prostě by jednoduše vyřadil všechna taková hesla *P'*, která by po provedení operace $D_{P'}(E_P(VA))$ vrátila jako výsledek sudé číslo. Takováto redukce prostoru hesel na polovinu zdánlivě nevypadá nijak nebezpečně. Uvážíme-li však, že při dalších sezeních jsou vždy vygenerovány nové hodnoty klíčů, lze tímto způsobem dále pokračovat v dělení/redukci prostoru hesel (celkově se tedy bude snižovat logaritmicky). Obecně se tento typ útoku, při němž dochází k postupnému dělení/redukci prostoru klíčů (hesel), nazývá *partition attack*.

Některé kryptosystémy jako například ElGamal mohou ale minimální dělení připustit – zde je pomocí hesla šifrováno nějaké celé číslo z intervalu $\langle 0, \beta - 1 \rangle$. Pokud jej zakódujeme do *n* bitů, tak budeme při zkoušení hesel schopni vyřadit všechna taková hesla *P'*, která po provedení operace $D_{P'}(E_P(VA))$ vrátí jako výsledek číslo z intervalu $\langle \beta, 2^n - 1 \rangle$. Zřejmě pokud

se $\beta$ bude blížit $2^n - 1$, tak bude možno vyloučit jen malý počet hesel. Naopak, hodnoty $\beta$ blízké $2^{n-1}$ povedou k velké redukci prostoru hesel.

Dále je také potřeba zvážit doplnění vstupních dat na odpovídající délku bloku podporovanou příslušným symetrickým algoritmem. Doplnění nulami s sebou přináší opět riziko útoku, a proto by tyto doplňující bity měly být raději náhodné.

Poslední dva výše zmíněné problémy lze efektivně vyřešit následující úpravou. Předpokládejme, že šifrujeme nějaké číslo modulo $\beta$ a délka šifrovacího bloku je $m$ bitů, kde $2^m > \beta$. Dále nechť $x = \lfloor 2^m/\beta \rfloor$ označuje číslo, kolikrát se interval $\langle 0, \beta - 1 \rangle$ vejde do jednoho bloku. Pak vždy zvolíme náhodnou hodnotu $j \in \langle 0, x - 1 \rangle$ a pomocí nemodulární aritmetiky přičteme k původnímu vstupnímu číslu hodnotu $j\beta$. Pokud je hodnota vstupního čísla menší než $2^m - x\beta$, použijeme $j \in \langle 0, x \rangle$.

Implementace základní části EKE pomocí DH metody ustavení klíčů se pak od obecného popisu protokolu mírně odklání – v prvních dvou krocích jsou přenášené hodnoty chráněny heslem a na jejich základě si pak nezávisle strana A i B vygeneruje klíč sezení (např. výběrem určitých bitů z $\alpha^{rArB} \bmod \beta$):

| A | | B |
|---|---|---|
| $E_P(\alpha^{rA} \bmod \beta)$ | $\rightarrow$ | |
| | $\leftarrow$ | $E_P(\alpha^{rB} \bmod \beta)$ |
| | … | |

Útočník bez znalosti hesla nemůže provést útok *man in the middle* ani výpočet diskrétního logaritmu (v případě malých hodnot $\beta$). Tuto implementaci EKE budeme většinou označovat jako DHEKE.

V [BM92] je dále diskutována volba vhodných (a)symetrických kryptosystémů, správných parametrů $\alpha$, $\beta$ a obrana proti kryptoanalytickým útokům.

# Reference


[BM92] S. M. Bellovin and M. Merritt. Encrypted Key Exchange: Password-based protocols secure against dictionary attacks. In Proceedings *IEEE Computer Society symposium on Research in Security and Privacy*, pages 72–84, May 1992.

[DH76] W. Diffie and M. E. Hellman. New Directions in Cryptography. In *IEEE Transactions on Information Theory*, volume IT-22, pages 644–654, November 1976.

[DvOW92] W. Diffie, P. C. van Oorschot, and M. J. Wiener. Authentication and Authenticated Key Exchange. In *Designs, Codes and Cryptography*, pages 107–125, 1992.

[PH78] S. C. Pohlig and M. E. Hellman. An improved algorithm for computing logarithms over GF(p) and its cryptographic significance. In IEEE, volume IT-24, pages 106–110, 1978.

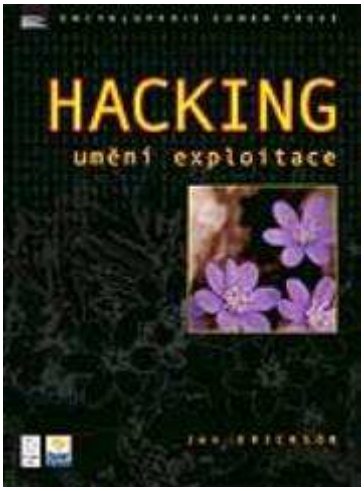
[vOW96] P. C. van Oorschot and M. J. Wiener. On Diffie-Hellman Key Agreement with Short Exponents. In *Advances in Cryptology – Eurocrypt 96*, volume 1070 of *Lecture Notes in Computer Science*, pages 332–343. Springer, 1996.

# F. Recenze knihy Jon Erickson: Hacking - umění exploitace

**(Jon Erickson: Hacking - umění exploitace, Zoner 2005, 264 str.)**

Autorem knihy je člověk, který vystupuje často na různých konferencích o počítačové bezpečnosti, pracuje jako kryptolog a bezpečnostní specialista v Severní Kalifornii (USA). Kniha vyšla v originále v roce 2003 (nakladatelství No Starch Press, ISBN 0-59327-007-0) a kromě českého překladu byla přeložena i do dalších jazyků (např. do polštiny a japonštiny). Třetí kapitolu této knihy, která se týká sítí, lze v originále stáhnout na této adrese http://mithras.itworld.com/download/book_chapters_and_wps/no_starch/hacking_ch3.pdf .

Kniha sestává z pěti kapitol - podstatou knihy jsou ale vlastně jen tři kapitoly, první kapitola je stručný úvod, pátá je stručný závěr.




Ukázky kódů v knize jsou vytvořeny na platformě x86 na operačním systému Linux. Čtenář s počítačem obdobné konfigurace má možnost experimentovat a ověřovat si výsledky na vlastní oči. V úvodní kapitole se autor zamýšlí nad podstatou pojmu "hacking", srovnává hacking a cracking. Co je na hackingu pozitivního a kde naopak jsou překračovány legislativní hranice?

Autor říká - cílem knihy je naučit čtenáře té pravé hackerské mentalitě - a samozřejmě tím míní to pozitivní, co hacking přináší pro ochranu systémů. Tam, kde je ochrana, tam jsou i útočníci a reálný svět se odvíjí ze vzájemné symbiózy.

Kapitola 2. nese název *Programování* a tvoří větší polovinu celé knihy. Autor vysvětluje, co se pro něho skrývá pod pojmy programování a exploitování programu. Program je sada pravidel, sledující nějaký tok činností, říká počítači, co má dělat. Exploitování programu pak znamená přinutit program, aby dělal to, co chci já (což může být třeba i opak toho, co zamýšlel původní programátor). Nejčastější typy exploitů využívají chybu přetečení paměti (buffer-overflow) a chybu ve formátovacím řetězci (format-string). Programátorovi někdy unikají hlubší souvislosti příkazů, které napsal, zatímco hacker zde stojí jaksi na vyšší úrovni a díky znalostem těchto souvislostí je schopný je využít pro své cíle. Autor pak uvádí celou řadu konkrétních příkladů.

Třetí kapitola se věnuje hackování sítí. Sítě - to je téma, které je především o komunikacích a k tomu existují pravidla, normy a protokoly. Výchozím základem je referenční model OSI, obsahující sedm vrstev. Autor vysvětluje princip odposlechů na síti, ukazuje, co jsou to aktivní odposlechy, co je to únos TCP/IP spojení, co je to útok DoS (Denial of Service) a celou řadu dalších postupů.

Čtvrtá kapitola má název kryptologie. Kromě vysvětlení základních principů kryptologie autor podrobněji popisuje útoky typu man-in-the-middle (na příkladu SSH spojení), zabývá se otázkami okolo lámání hesel (slovníkové útoky, vyhledávací tabulky hashů, útok time/trade space-off). V posledních částech kapitoly se autor věnuje bezdrátovým sítím (útoky proti WEP - Wired Equivalent Privacy).

V páté závěrečné kapitole autor vyslovuje myšlenku, se kterou nelze jinak než souhlasit - bez hackingu by slabiny v programech zůstaly neobjevené.

Kniha má jeden velice pozitivní rys, lze ji doporučit i méně technicky orientovanému čtenáři, autorovo objasňování problematiky je srozumitelné, zřejmé a přitom dostatečně detailní.

Jaroslav Pinkava, PVT a.s. (jaroslav.pinkava@pvt.cz)

# G. O čem jsme psali v červnu 2000 – 2004

# H. Závěrečné informace

## 1. Sešit

Crypto-World je oficiální informační sešit "Kryptologické sekce Jednoty českých matematiků a fyziků" (GCUCMP). Obsahuje články podepsané autory. Případné chyby a nepřesnosti jsou dílem P.Vondrušky a autorů jednotlivých podepsaných článků, GCUCMP za ně nemá odbornou ani jinou zodpovědnost.

Adresa URL, na níž můžete najít tento sešit (zpravidla 3 týdny po jeho rozeslání) a předchozí sešity GCUCMP, denně aktualizované novinky z kryptologie a informační bezpečnosti, normy, standardy, stránky některých členů a další související materiály:

http://crypto-world.info

## 2. Registrace / zrušení registrace

Zájemci o e-zin se mohou zaregistrovat pomocí e-mailu na adrese pavel.vondruska@crypto-world.info (předmět: Crypto-World) nebo použít k odeslání žádosti o registraci elektronický formulář na http://crypto-world.info. Při registraci vyžadujeme pouze **jméno a příjmení, titul**, pracoviště (není podmínkou) a **e-mail adresu** určenou k zasílání kódů ke stažení sešitu.

Ke **zrušení registrace** stačí zaslat krátkou zprávu na e-mail pavel.vondruska@crypto-world.info (předmět: ruším odběr Crypto-Worldu!) nebo opět použít formulář na http://crypto-world.info. Ve zprávě prosím uveďte jméno a příjmení a **e-mail adresu**, na kterou byly kódy zasílány.

## 3. Redakce

**E-zin Crypto-World**

| | |
|---|---|
| Redakční práce: | Pavel Vondruška |
| Stálí přispěvatelé: | Pavel Vondruška |
| | Jaroslav Pinkava |
| Jazyková úprava: | Jakub Vrána |
| Přehled autorů: | http://crypto-world.info/obsah/autori.pdf |

| | |
|---|---|
| **NEWS** | Vlastimil Klíma |
| (výběr příspěvků, | Jaroslav Pinkava |
| komentáře a | Tomáš Rosa |
| vkládání na web) | Pavel Vondruška |

**Webmaster** Pavel Vondruška, jr.

## 4. Spojení (abecedně)

| | | |
|---|---|---|
| **redakce e-zinu** | ezin@crypto-world.info , | http://crypto-world.info |
| Vlastimil Klíma | v.klima@volny.cz , | http://cryptography.hyperlink.cz/ |
| Jaroslav Pinkava | jaroslav.pinkava@pvt.cz , | http://crypto-world.info/pinkava/ |
| Tomáš Rosa | t_rosa@volny.cz , | http://crypto.hyperlink.cz/ |
| Pavel Vondruška | pavel.vondruska@crypto-world.info , | http://crypto-world.info/vondruska/index.php |
| Pavel Vondruška,jr. | pavel@crypto-world.info , | http://webdesign.crypto-world.info |
| Jakub Vrána | jakub@vrana.cz , | http://www.vrana.cz/ |